METHOD, NODE AND COMPUTER READABLE MEDIUM FOR PERFORMING MULTIPLE SIGNATURE MATCHING IN AN INTRUSION PREVENTION SYSTEM

ABSTRACT OF THE INVENTION

A node of a network maintaining an instance of an intrusion prevention system, the node comprising a memory module for storing data in machine-readable format for retrieval and execution by a central processing unit and an operating system comprising a network stack comprising a protocol driver, a media access control driver and an instance of the intrusion prevention system implemented as an intermediate driver and bound to the protocol driver and the media access control driver, the intrusion prevention system comprising an associative process engine and an input/output control layer, the input/output control layer operable to receive at least one of a plurality of machine-readable network-exploit signatures from a database and provide the at least one machine-readable network-exploit signatures to the associative process engine, the associative process engine operable to compare a packet with the at least one machine-readable network-exploit signature and determine a correspondence between the packet and the at least one machine-readable network-exploit signature is provided. A method of analyzing a packet at a node of a network by an intrusion prevention system executed by the node comprising reading the packet by the intrusion prevention system, comparing the packet with a plurality of machine-readable network-exploit signatures, and determining a correspondence between the packet and at least two of the plurality of machine-readable network-exploit signatures is provided. A computer-readable medium having stored thereon a set of instructions to be executed, the set of instructions, when executed by a processor, cause the processor to perform a computer method of comparing a packet with a plurality of machine-readable network-exploit signatures, determining a correspondence between the packet and at least a subset of the plurality of machine-readable network-exploit signatures, and generating a record with which the correspondence is made.